REMARKS

Claims 1-3 and 6-8 are pending in the application and stand rejected.

Rejection under 35 U.S.C §102

Claims 1-3 and 6-8 stand rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,853,988 to Dickinson. In particular, the Examiner finds that, with regard to claim 1, Dickinson discloses all of the claimed limitations. Applicants have reviewed the reference with care, paying particular attention to the passages cited, and are compelled to respectfully disagree with the Examiner's characterization of this reference. Briefly, Dickinson provides a central, network-accessible server that offers cryptographic services to users; the main novelty of Dickinson lies in that all cryptographic keys of the various users are stored on the server and never leave the server, as all cryptographic services (encrypting, decrypting, authentication, authorization, digital signing, etc.) are performed exclusively on the server itself. As previously noted, the presently claimed invention is directed to a method wherein a third party is interacting on behalf of a user (pretending, essentially, to be the user) with another, suspect, party as part of investigating that suspect party. It is quite clear that Dickinson and the presently claimed invention really have nothing in common.

With greater specificity, the Examiner asserts that Dickinson discloses an investigation agency selecting a user within the trusted computing environment at col. 3 ll. 14-19 and 60-67; the investigation agency obtaining consent from the selected user to use an identity of the user in an investigation of a suspect party at col. 7 ll. 43-49 and col. 2 ll. 36-41; the investigation agency creating an investigation identity which that is owned by the user at col.7 ll. 53-59; the investigation agency using the investigation identity to take part in transactions with the suspect party col. 8 ll. 4-6; and creating a record of those transactions at col. 12 ll. 22-24 and 27-30. Applicants submit that this is in fact an incorrect reading of Dickinson.

At col. 3 ll. 14-19 and 60-67 Dickinson teaches nothing more than:

> The method further comprises associating a user from multiple users with one or more keys from a

> plurality of private cryptographic keys stored on a secure server and receiving a request for one or more cryptographic functions from an application executing on a remote computing device.
>
> ...
>
> The one or more keys are associated with a user. The method comprises storing one or more private keys on a server, receiving a request for a cryptographic action, and determining a type of certificate that corresponds to the cryptographic action. The method also comprises determining whether a user has access to a certificate matching the type, and when the user has access to the certificate, performing the cryptographic action using one or more of the private keys that correspond to the certificate.

Where in these paragraphs does the Examine discern any teaching regarding an investigation agency? A trusted computing environment? An investigation agency selecting a user within a trusted computing environment?

At col. 7 ll. 43-49 and col. 2 ll. 36-41 Dickinson teaches:

> Once the user produces the appropriate authentication data and the trust engine 110 determines a positive match between that authentication data (current authentication data) and the authentication data provided at the time of enrollment (enrollment authentication data), the trust engine 110 provides the user with complete cryptographic functionality. For example, the properly authenticated user may advantageously employ the trust engine 110 to perform hashing, digitally signing,

> encrypting and decrypting (often referred to only as encrypting), creating or distributing digital certificates, and the like. However, the private cryptographic keys used in <u>the cryptographic functions will not be available outside the trust engine</u> 110, thereby ensuring the integrity of the cryptographic keys.
>
> ...
>
> According to this embodiment, a user accesses the trust engine in order to exercise cryptographic functions, such as, for example, authentication, authorization, digital signing and certificates, encryption, notary-like and power-of-attorney-like actions, and the like.

It is clear from these passages that all interaction is between the user and the trusted server <u>only</u>. Furthermore, where in these passages does the Examiner find any mention of the investigation agency obtaining <u>consent</u> from the selected user to use an identity of the user in an investigation of a suspect party? What does the Examiner understand to correspond to the claimed identity of the user? Who is the suspect party?

At col.7 ll. 53-59 Dickinson teaches:

> According to one embodiment, the trust engine 110 generates and stores cryptographic keys. According to another embodiment, at least one cryptographic key is associated with each user. Moreover, when the cryptographic keys include public-key technology, each private key associated with a user is generated within, <u>and not released from</u>, the trust engine 110.

Where does the Examiner discern a teaching of an investigation agency creating an investigation *identity* which that is *owned by a user*? A cryptographic key is <u>not</u> an identity of a user. Furthermore, the cryptographic key is not owned by the user, merely *associated* with that user – this is abundantly clear from the above passage: "each private key associated with a user is generated within, and not released from, the trust engine."

At col. 8 ll. 4-6 Dickinson teaches that:

> ...the trust engine 110 uses its own cryptographic key pair to perform cryptographic functions on behalf of the authenticated user.

Once again, how is this the same as an investigation agency using the investigation identity to take part in transactions with a suspect party? Who is the suspect party? Where are the transactions? The cryptographic functions, as has been made abundantly clear, are all performed exclusively on the server (trust engine) and thus cannot possibly be viewed as corresponding to transactions carried out with a third party (the suspect party).

Finally, at col. 12 ll. 22-24 and 27-30 Dickinson teaches:

> As mentioned in the foregoing, the transaction engine 205 keeps data corresponding to an audit trail and stores such data in the mass storage 225... The depository audit trail data is similar to that of the transaction engine 205 in that the audit trail data comprises a record of the requests received by the depository 210 and the response thereof.

How is this the same creating a record of transactions carried out on behalf of a user by an investigation agency with a suspect third party?

Applicants submit that Dickinson is in fact irrelevant to the presently claimed invention because, as shown above, Dickinson fails to disclose any of the limitations of claim 1. Applicants therefore respectfully submit that claim 1 is in fact patentable over Dickinson and request the Examiner to kindly reconsider and allow this claim, or else to clearly and specifically point out where Dickinson discloses each and every claimed feature as discussed above, in accordance with 37 C.F.R. 1.104(c)2.

Claims 2-3 and 6-8 depend from claim 1. In view of the above discussion, it is submitted that claim 1 is allowable, and for this reason claims 2-3 and 6-8 are also allowable and are not individually addressed elsewhere herein.

In view of the above, Applicants submit that the application is now in condition for allowance and respectfully urge the Examiner to pass this case to issue.

The Commissioner is authorized to charge any additional fees which may be required or credit overpayment to deposit account no. 08-2025. In particular, if this response is not timely filed, the Commissioner is authorized to treat this response as including a petition to extend the time period pursuant to 37 CFR 1.136(a) requesting an extension of time of the number of months necessary to make this response timely filed and the petition fee due in connection therewith may be charged to deposit account no. 08-2025.

I hereby certify that this correspondence is being deposited with the United States Post Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

March 1, 2006
(Date of Transmission)

Alma Smalling
(Name of Person Transmitting)

(Signature)

3/1/06
(Date)

Respectfully submitted,

Robert Popa
Attorney for Applicants
Reg. No. 43,010
LADAS & PARRY
5670 Wilshire Boulevard, Suite 2100
Los Angeles, California 90036
(323) 934-2300 voice
(323) 934-0202 facsimile
rpopa@ladasparry.com